

$$\underline{RS} = \begin{pmatrix} 01 & a4 & 55 & 87 & 5a & 58 & db & 9e \\ a4 & 56 & 82 & f3 & 1e & c6 & 68 & e5 \\ 02 & a1 & fc & c1 & 47 & ae & 3d & 19 \\ a4 & 55 & 87 & 5a & 58 & db & 9e & 03 \end{pmatrix}$$

$$\begin{pmatrix} S_{i,0} \\ S_{i,1} \\ S_{i,2} \\ S_{i,3} \end{pmatrix} = \underline{RS} \cdot \begin{pmatrix} m_{8i+0} \\ m_{8i+1} \\ \dots \\ m_{8i+6} \\ m_{8i+7} \end{pmatrix} \quad (1)$$

$$S_i = \sum_{j=0}^3 s_{i,j} \cdot 2^{8j} \quad i = 0, 1, \dots, k-1$$

$$S = (S_{k-1}, S_{k-2}, \dots, S_1, S_0)$$